NetIQ® Identity Manager™

Driver for Workday Implementation Guide

June 2016

Legal Notices

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2014 NetIQ Corporation. All Rights Reserved.

For information about NetIQ trademarks, see https://www.netiq.com/company/legal/

Contents

About this Book and the Library **4**

About NetIQ Corporation **5**

1 Understanding the Workday Driver **7**

1.1 Driver Concepts 7
1.1.1 Data Management 7
1.1.2 How the Driver Works 8
1.2 Support for Standard Driver Features 10
1.2.1 Local Platforms 10
1.2.3 Supported Operations 11

2 Installing the Driver Files **13**

3 Creating a New Driver Object **14**

3.1 Creating the Driver Object in Designer 14
3.1.1 Importing the Current Driver Packages 15
3.1.2 Installing the Driver Packages 15
3.1.3 Configuring the Driver Object 19
3.1.4 Deploying the Driver Object 29
3.1.5 Starting the Driver 30
3.2 Activating the Driver 30
3.3 Adding Packages to an Existing Driver 30

4 Schema Mapping & filter settings **32**

4.1 Schema Mapping 32
4.1 Filter Settings 37

5 Securing Communication **42**

6 Managing the Driver **43**

7 Troubleshooting the Driver **44**

8.1 Driver Shim Errors 44
8.2 Driver Cache file and Driver State settings: 44
8.3 Troubleshooting Driver Processes 45
8.4 Migrating Individual Object from Workday 46

(A) Driver Properties **49**

A.1 Driver Configuration 49
A.1.1 Driver Module 49
A.1.2 Driver Object Password 50
A.1.3 Authentication 50
A.1.4 Startup Option 51
A.1.5 Driver Parameters 51

(B) Trace Level **53**

(C) IDV Schema extension: **54**

(D) IDV proposed structure: **54**

About this Book and the Library

The *Identity Manager Driver for Workday Implementation Guide* explains how to install and configure the Identity Manager Driver for Workday.

Intended Audience

This book provides information for individuals responsible for using the Identity Manager Driver for Workday. You should also have an understanding of SOAP, HTML, and HTTP protocols.

Other Information in the Library

The library provides the following information resources:

Identity Manager Setup Guide

Provides overview of Identity Manager and its components. This book also provides detailed planning and installation information for Identity Manager.

Designer Administration Guide

Provides information about designing, testing, documenting, and deploying Identity Manager Solutions in a highly productive environment.

User Application: Administration Guide

Describes how to administer the Identity Manager User Application.

User Application: User Guide

Describes the user interface of the Identity Manager User Application and how you can use the features it offers, including identity self-service, the Work Dashboard, role and resource management, and compliance management.

User Application: Design Guide

Describes how to use the Designer to create User Application components, including how to work with the Provisioning view, the directory abstraction layer editor, the provisioning request definition editor, the provisioning team editor, and the role catalog.

Identity Reporting Module Guide

Describes the Identity Reporting Module for Identity Manager and how you can use the features it offers, including the Reporting Module user interface and custom report definitions, as well as providing installation instructions.

Analyzer Administration Guide

Describes how to administer Analyzer for Identity Manager.

Identity Manager Common Driver Administration Guide

Provides information about administration tasks that are common to all Identity Manager Drivers.

Identity Manager Driver Guides

Provides implementation information about Identity Manager Drivers.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate—day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with—for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ Web site in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **Add Comment** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit community.netiq.com.

1 Understanding the Workday Driver

Identity Manager 4.0 and later offers automatic provisioning and synchronization of users to cloud applications. The new Workday driver for NetIQ Identity Manager can seamlessly provision and de-provision users from the Workday cloud application, keeping the user identity information consistent across the Identity Vault and can also update some IDV authoritative attributes such as User ID, Email address etc. back to the cloud application. The Workday driver can supports secure password synchronization across Identity Vault to Workday cloud and supports seamless and configurable automatic user provisioning in IDV.

The Workday driver uses a combination of language and protocols to enable identity provisioning and data synchronization between Identity Vault and Workday.

IMPORTANT: The Workday driver shim is supported on IDM4.5 and above but can be used with IDM4.0 with Remote loader at IDM4.5 and above. The driver support Workday version v25.0 onwards.

This section provides the following information on the Workday driver:

- Section 1.1, "Driver Concepts," on page 9
- Section 1.2, "Support for Standard Driver Features," on page 11

1.1 Driver Concepts

Use the information in this section to understand the driver concepts:

- "Data Management" on page 9
- "How the Driver Works" on page 10

1.1.1 Data Management

The Workday driver communicates with Workday using the Workday SOAP API specially Human_Resource API. Some of the important Human resource API used in the driver are as follow:

- Get_Workers
- Get_Worker_Photos
- Get_Locations
- Get_Organizations
- Get_Job_Profiles
- Get_Job_Families
- Change_Personal_Information

- Update_Workday_Account
- Maintain_Contact_Information

The Human_Resource API is represented as XML and its transport is SOAP 1.1 over HTTPS.

- "SOAP" on page 10
- "XML" on page 10
- "HTTP" on page 10

SOAP

SOAP (Simple Object Access Protocol) is an XML-based protocol for exchanging messages. It defines the message exchange but not the message content. The driver supports SOAP 1.1.

SOAP documents are organized into three elements:

- **Envelope:** The root XML node.
- **Header:** Provides context knowledge such as a transaction ID and security information.
- **Body:** The method-specific information.

SOAP follows the HTTP request/response message model, which provides SOAP request parameters in an HTTP request and SOAP response parameters in an HTTP response.

XML

XML (Extensible Markup Language) is a generic subset of Standard Generalized Markup Language (SGML) that allows for exchange of structured data on the Internet.

HTTP

HTTP is a protocol used to request and transmit data over the Internet or other computer network. The protocol works well in an Internet infrastructure and with firewalls.

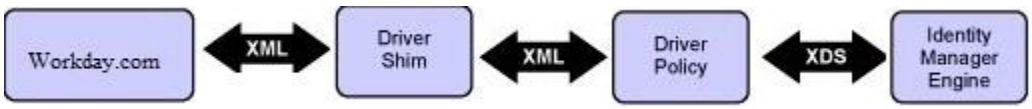
HTTP is a stateless request/response system because the connection is usually maintained only for the immediate request. The client establishes a TCP connection with the server and sends it a request command. The server then sends back its response.

NOTE: Workday communication mostly happens over HTTPS.

1.1.2 How the Driver Works

The following diagram illustrates the data flow from Workday service to Identity Manager:

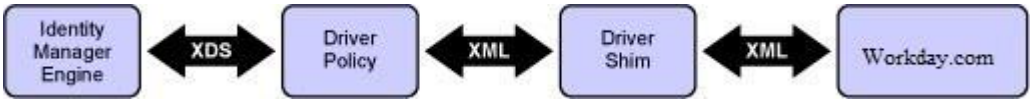
Figure 1-1 *Workday Driver Data Flow*



The Identity Manager engine polls the data as one time initial migration from workday as Soap request. Workday processes the request, and returns a SOAP response to the driver shim. The

driver processes the response, converting it into appropriate XDS that is reported back to the Identity Manager engine. The Publisher channel periodically polls for additions and modifications to the objects in Workday. On a successful retrieval of the changes, it stores the polling time for use in the next polling cycle. To prevent loopback, the driver discards modifications done by users that the Subscriber channel uses to update Workday.

The following diagram illustrates the data flow from Identity Manager to Workday service:



The Identity Manager engine uses XDS, a specialized form of XML, to represent events in the Identity Vault. Identity Manager passes the XDS to the driver policy, which can consist of basic policies, DirXML Script, and XSLT style sheets. The driver shim receives the XML from the driver policy. The driver shim uses SOAP to communicate with Workday.

1.2 Support for Standard Driver Features

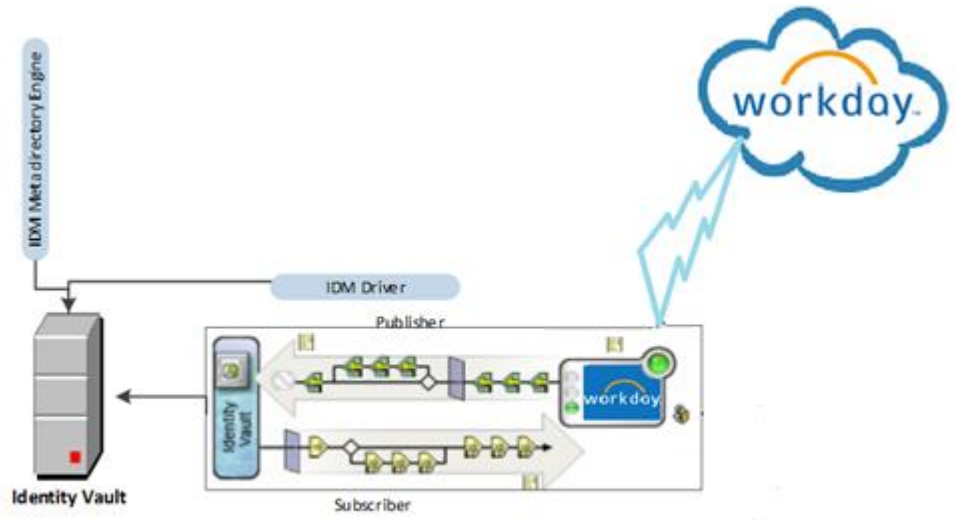
The following sections provide information about how the Workday driver supports these standard driver features:

- Section 1.2.1, "Local Platforms," on page 11
- Section 1.2.2, "Remote Platforms," on page 11
- Section 1.2.3, "Supported Operations," on page 11

1.2.1 Local Platforms

Installation of the driver on the Metadirectory server is known as local installation. You can install the Workday driver on the operating systems supported for the Metadirectory server.

For information about the operating systems supported for the Metadirectory server, see "Considerations for Installing Drivers with the Identity Manager Engine" in the *NetIQ Identity Manager Setup Guide*.

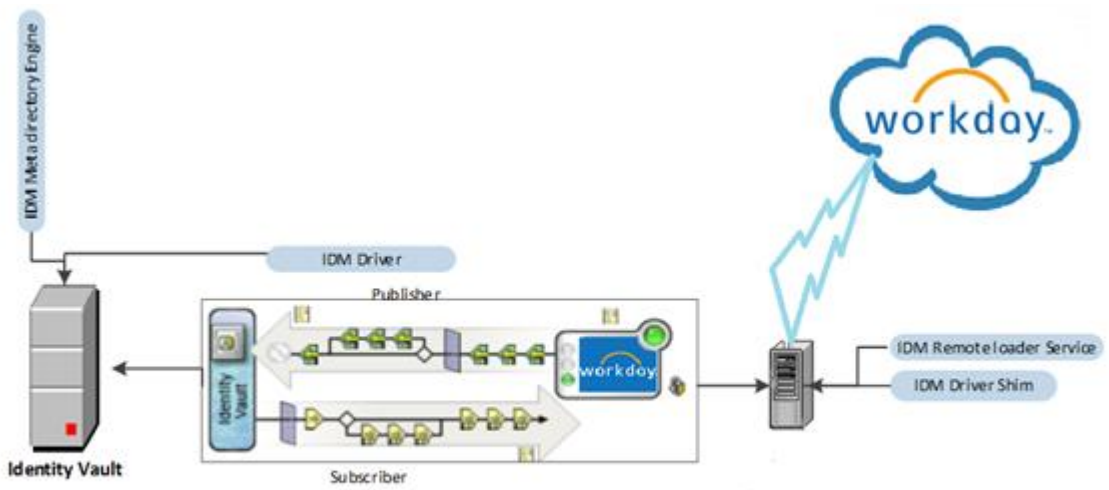


Workday Driver architecture with local platforms

1.2.2 Remote Platforms

The Workday driver can use the Remote Loader service to run on a server other than the Metadirectory server. You can install the Workday driver on the operating systems supported for the Remote Loader.

For information about the supported operating systems, see *System Requirements for the Remote Loader* in the *NetIQ Identity Manager Setup Guide*.



Workday Driver architecture with Remote platforms

1.2.3 Supported Operations

The Workday driver supports the following operations on the Subscriber channel

- Update user ID: When a user is created or renamed in IDV, then the driver update the user ID back in the Workday.
- Update user's attribute such as email Address in IDV: When a user is updated in IDV, the updated user information can be synchronized with the Workday.
- Delete users: Delete event is not allowed in the workday, so event is being vetoed.
- Password synchronization: The Workday driver is capable of synchronizing password from IDV to workday. However, this has not yet been implemented. The password cannot be synchronized from workday to IDV

NOTE: Workday driver does not support the following:

- User creation in workday (Left for next release)
- Multivalued attributes. If multivalued attributes are added to the Identity Vault, only one of the values is synchronized with the Workday driver.

The following operations are supported on the Publisher channel:

- Users Object:
  - Add users (Employee and Contingent Worker Both)
  - Modify users: When a user is updated in Workday, the updated user information is synchronized with the IDV.
  - Delete users: Users is not deleted in Workday, so no delete event from workday.
- Position or Relation object: Each job /position is treated as a relation irrespective of primary position or non-primary position. The primary position is also synchronized to the user object.
- Location Object: Driver synchronizes locations and creates a separate object in IDV.

- Job Family Object: Driver synchronizes job Family and creates a separate object in IDV.
- Job Profile Object: Driver synchronizes job profile and creates a separate object in IDV.
- Organization Object: Driver synchronizes organizations and creates a separate object in IDV.
  NOTE: Organization is configurable and can have different values such as Cost Center, Company, and HR Company etc.
- Photo: Driver can also poll worker's photo from workday.

2 Installing the Driver Files

You must install Workday driver on a server that has HTTP access to the Workday Web service. It requires to communicate with the web service for polling and updating the identity data. The Workday driver can be installed on multiple systems and platforms. To verify the system requirement list, see "System Requirements for the Identity Manager Engine" in the *NetIQ Identity Manager Setup Guide*.

By default, the Workday driver files are installed on the Metadirectory server at the same time as the Metadirectory engine. The driver can also be installed using remote loader on windows server.

NOTE: The extension of Identity Vault's schema is required before installing the driver shim.

3 Creating a New Driver Object

After the Workday driver files are installed on the server where you want to run the driver (see Chapter 2, "Installing the Driver Files," on page 13), you can create the driver in the Identity Vault. You can achieve this by installing the driver packages or importing the driver configuration file and then modifying the driver configuration to suit your environment. The following package are created for this driver:

- Workday Base : Base Package
- Workday Default Configuration : For User Object
- Workday Position Relation : For Relation object
- Workday Job Profile Synchronization : For Job Profile object
- Workday Job Family Synchronization : For Job Family Object
- Workday Location Synchronization : For Location Object
- Workday Organization Synchronization: For Organization Object including Cost Center, Company and HR Company etc.
- Workday Photo synchronization: For User's Photo.
- Workday Custom Package: Company specific customization.

The following sections provide instructions on how to create the driver:

- Section 3.1, "Creating the Driver Object in Designer," on page 15
- Section 3.2, "Activating the Driver," on page 20
- Section 3.3, "Adding Packages to an Existing Driver," on page 20

3.1 Creating the Driver Object in Designer

To create a Workday driver object, you need to install the driver packages and then modify the configuration to suit your environment. After you create and configure the driver object, you need to deploy it to the Identity Vault and start it.

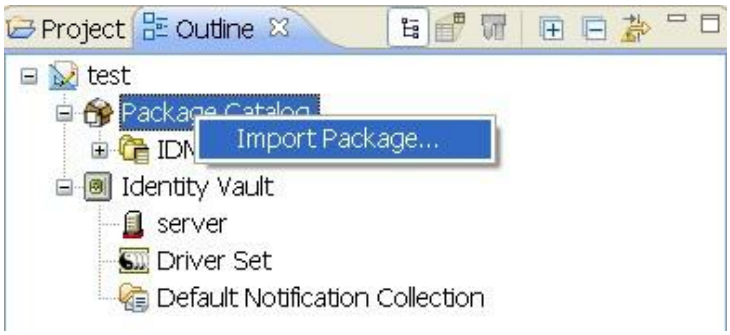
- Section 3.1.1, "Importing the Current Driver Packages," on page 15
- Section 3.1.2, "Installing the Driver Packages," on page 16
- Section 3.1.3, "Configuring the Driver Object," on page 18
- Section 3.1.4, "Deploying the Driver Object," on page 19
- Section 3.1.5, "Starting the Driver," on page 20

3.1.1 Importing the Current Driver Packages

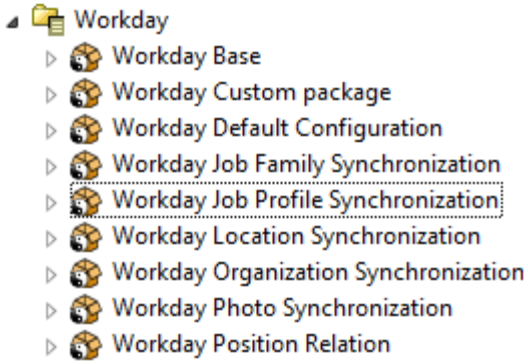
The driver packages contain the items required to create a driver, such as policies, entitlements, filters, and Schema Mapping policies. These packages are only available in Designer and can be updated after they are initially installed. You must have the most current version of the packages in the Package Catalog before you can create a new driver object.

To verify that you have the most recent version of the driver packages in the Package Catalog:

1. Launch Designer.
2. Browse to *Help* > *Check for Package Updates* in the toolbar.
3. Click *OK* to update the packages or
   Click *OK* if the packages are up-to-date.
4. In the Outline view, right-click the Package Catalog.
5. Click *Import Package*.



6. Select any Workday driver packages or
   Click *Select All* to import all of the packages displayed.
   By default, only the base packages are displayed. Deselect *Show Base Packages Only* to display all packages.
7. Click *OK* to import the selected packages, then click *OK* in the successfully imported packages message.



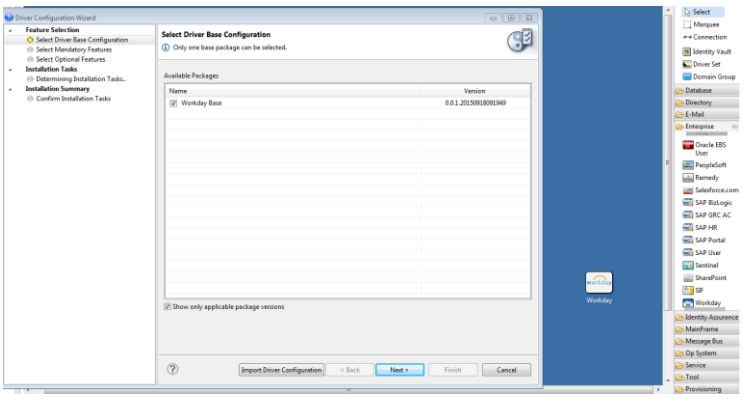
8. After the current packages are imported, continue with Section 3.1.2, "Installing the Driver Packages," on page 16.

3.1.2 Installing the Driver Packages

1. In Designer, open your project.
2. From the Palette, drag-and-drop the Workday driver to the desired driver set in the Modeler.

The Workday driver is listed under the Enterprise category in the Palette.

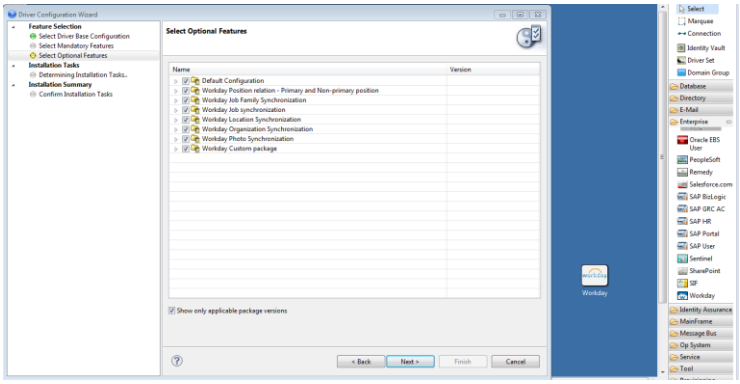
3 Select *Workday Base*, then click *Next*.



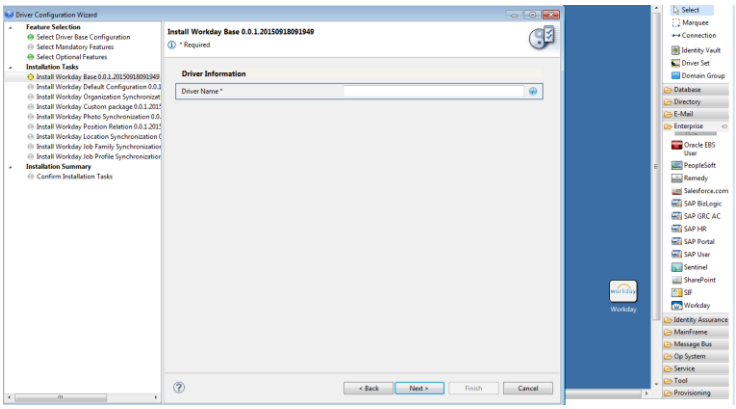
4 Select the optional features to install for the Workday driver, then click *Next*.

All options are selected by default. The options are:

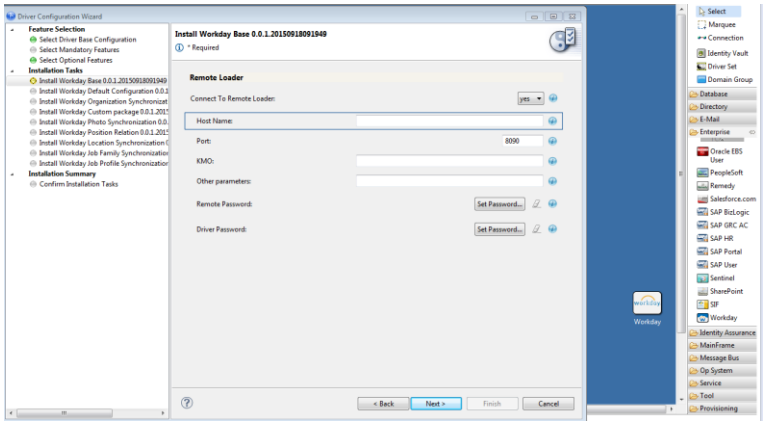
Default Configuration: These packages contain the default configuration information for the Workday workers (users). Always leave this option selected.



5 Fill The Driver Name fields, then click Next:



6 Select the remote loader option (Yes/No) and fill the remote loader fields Host Name, Port, KMO, Other parameters and set the Remote password and Driver Password. Click *Next*.



7 On the new Install Workday Base page, enter details in the following fields and click *Next*:

Workday Login ID: Specify the e-mail address used to login to Workday.

Authentication Type: Basic

Workday Login URL: Specify the login URL of Workday.

Workday Version: v25.0 (support v25.0) onwards

Set Proxy Authentication parameter: Proxy Host and port, User ID and password.

Ensure that you create a unique administrator user to be solely used by the Workday driver for authentication and specify that user in this parameter. If you specify the same user with which you login and administer Workday, the driver ignores the changes made on the Publisher channel (loopback detection).

Publisher Option:

(A) Select Show for details and select the following under Recurring API

- **Poll Worker:** Enable/Disable
- **Poll Job Profile:** Enable/Disable
- **Poll Interval :** Suggested interval is 10 minutes

(B)Select Show for details and select the following under Scheduled API

- **Poll Location:** Enable/Disable
- **Poll Worker Photo:** Enable/Disable
- **Poll Job Family:** Enable/Disable
- **Poll Organization:** Enable/Disable
- **Scheduler :** Set Time of the day to run the batch job
- **Publisher Heart Beat Interval:** Default value is 10 minutes

(C) Do not disturb the Parameter Name. Provide the parameter value as follows:

- **Parameter wdOrgList:** Organization Subcategory in the Workday. Default values are COST_CENTER, COMPANY, HR_COMPANY (it is a configurable item, so check with Workday administrator)
- **Parameter wdVersion:** Required for Query on publisher channel. Provide the Version of Workday.

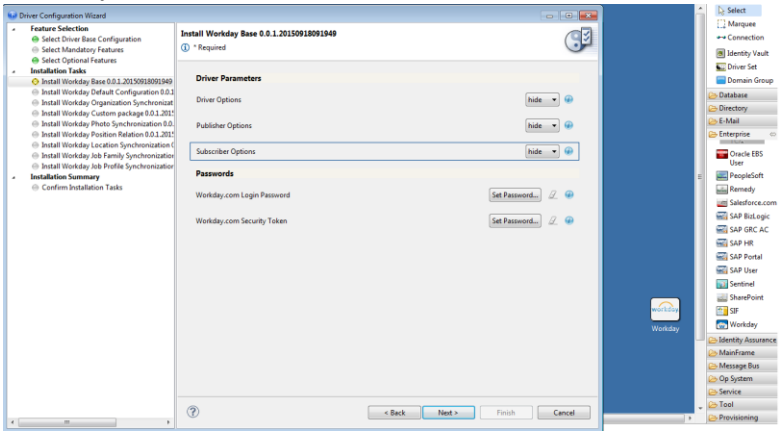
Subscriber Option:

(A) Do not disturb the Parameter Name. Provide the parameter value as follows:

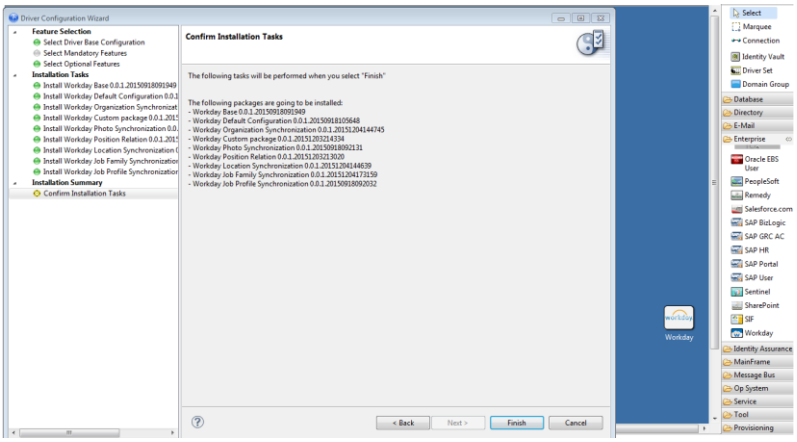
- **Parameter wdOrgList:** Organization Subcategory in the Workday. The default values are COST_CENTER, COMPANY, HR_COMPANY (it is a configurable item. Check with Workday administrator)
- **Parameter wdVersion:** Required for Query on subscriber channel. Provides the Version of Workday.
- **Parameter wdWorkerListInclude:** Required for Query on subscriber channel for worker. Check with Workday administrator before changing it.
- **Parameter wdWorkerListExclude:** Required for Query on subscriber channel for worker. Check with Workday administrator before changing it.

Password Option: Under Password section, provide the following details:

- **Workday Login Password:** Specify the authentication password to login to Workday
- **Workday Security Token:** Specify the security token for login account at Workday



12 Review the summary of tasks completed to create the driver and click *Finish*.



13 After you have installed the driver, you can change the configuration for your environment. Proceed to Section 3.1.3, "Configuring the Driver Object," on page 18.

or

If you do not need to configure the driver, continue with Section 3.1.4, "Deploying the Driver Object," on page 19.

3.1.3 Configuring the Driver Object

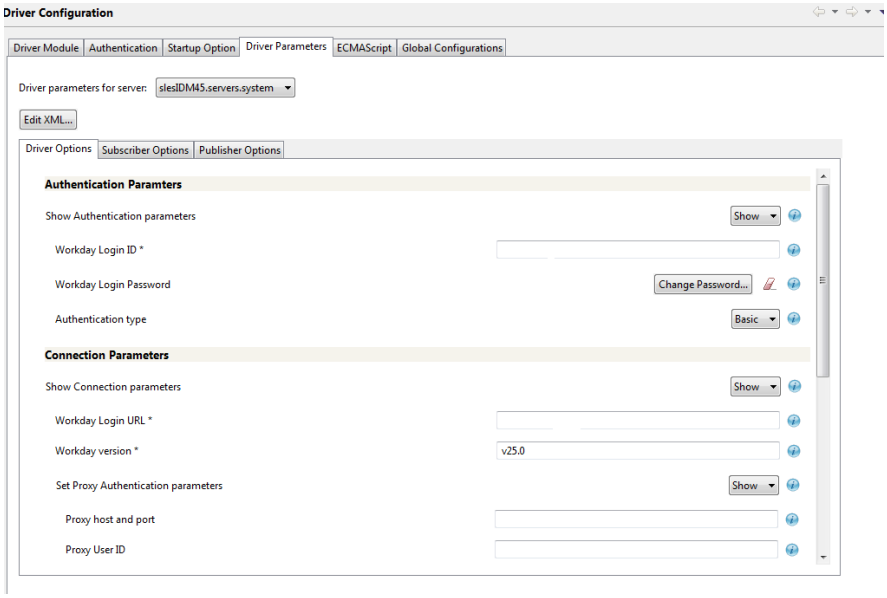
There are many settings that can help you customize and optimize the driver. You should complete the following tasks to configure the driver:

Configure the driver parameters: There are many settings that can help you customize and optimize the driver. The settings are divided into categories such as Driver Configuration, Engine Control Values, and Global Configuration Values (GCVs). Although it is important for you to understand all of the settings, you must first review the Driver Parameters located on the Driver Configuration page. The Driver Parameters lets you to configure the Workday login information and security credentials, and other parameters associated with the Publisher channel.

3.1.3.1 Driver Configuration- Engine Control Values:

These option are designed for the driver shim to poll the data from Workday.

- **Driver Configuration - Driver Options**



Workday Login ID: Specify the user ID to login to Workday (System ID to access the workday system through SOAP API).

Workday login Password: Specify the authentication password to login to Workday.

Authentication Type: Select authentication type (Available option is 'Basic')

Workday Login URL: Specify the login URL of Workday. For example:

'https://wd-impl-services.Workday/ccx/service/abccompany/Human_Resources/v25.0'

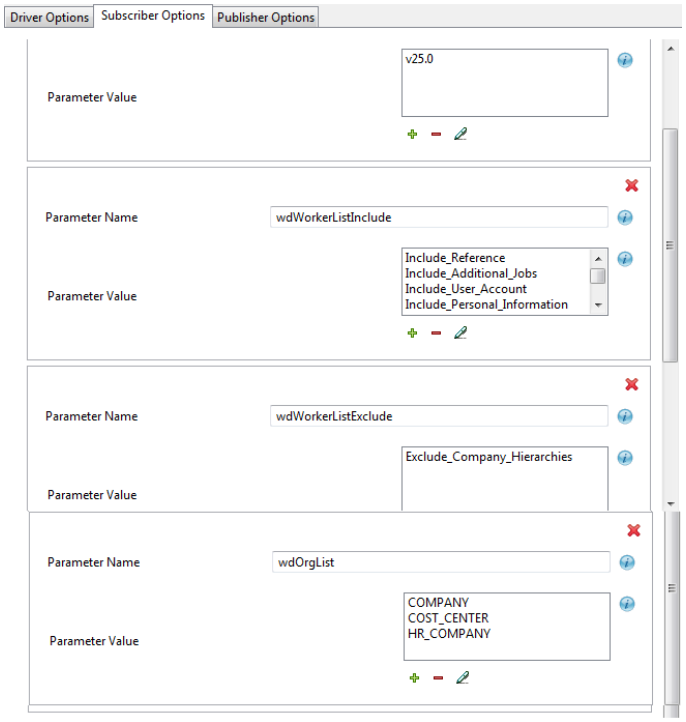
Workday version: Specify the API version of workday. Current supported version is v25.0

Proxy Host and Port: When an HTTP proxy is used, specify the host address and the host port. For example: 192.10.1.3:18180. Else, leave this field blank.

Proxy User ID: Specify the username of proxy user for authentication. Leave this field blank for anonymous authentication.

Proxy User Password: When a proxy user authentication is used, specify the password of the user.

☐ Driver Configuration – Subscriber Options



Transformation parameters are used for soap call on subscriber channel.

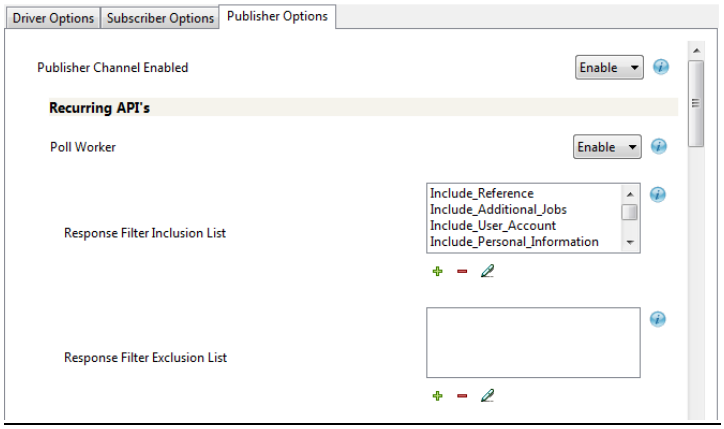
- Parameter Name: wdVersion (Do not change it)
  Value: Workday version: for Example v25.0
- Parameter Name: wdWorkerListInclude (Do not change it) used for poll /query/query-ex worker from workday on subscriber channel.
  Value: Default value for GET_WORKER API are
  - `Include_Reference`
  - `Include_Additional_Jobs`
  - `Include_User_Account`
  - `Include_Personal_Information`
  - `Include_Employment_Information`
  - `Include_Organizations`
  - `Exclude_Organization_Support_Role_Data`
  - `Exclude_Location_Hierarchies`
  - `Exclude_Cost_Center_Hierarchies`
  - `Exclude_Matrix_Organizations`
  - `Exclude_Supervisory_Organizations`
  - `Include_Roles`

  Drop and add option as per requirement.
- Parameter Name: wdOrgList (Do not change it)
  Value: Organization Type (Configurable item in workday- Need to configure as per workday installation)
  - `COMPANY`
  - `COST_CENTER`
  - `HR_COMPANY`

☐ **Driver Configuration – Publisher Options : Polling of the workday information is divided under two broad categories:**

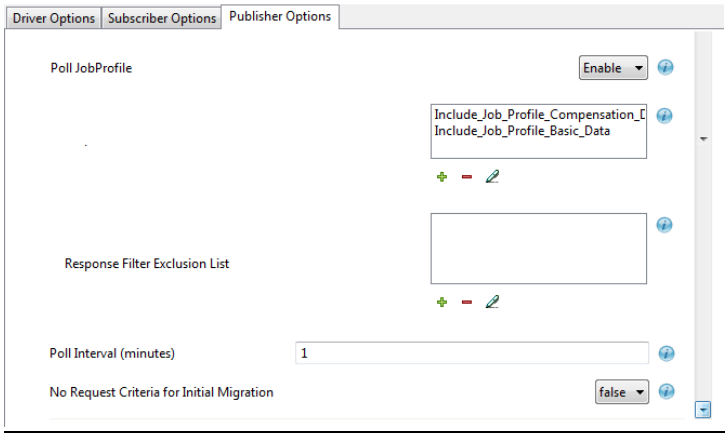
- **Recurring API:** based on workday API which allow to poll the data such as worker and job profile, on basis of workday transition log. In this case polling the data changed in certain interval is possible.

a. Polling Worker



- Poll Worker: Select enable for polling the worker information.
- Response Filter Inclusion List: The default option to pull the worker are as follows: you may skip this option if you do not need any information.
  - `Include_Reference`
  - `Include_Additional_Jobs`
  - `Include_User_Account`
  - `Include_Personal_Information`
  - `Include_Employment_Information`
  - `Include_Organizations`
  - `Exclude_Organization_Support_Role_Data`
  - `Exclude_Location_Hierarchies`
  - `Exclude_Cost_Center_Hierarchies`
  - `Exclude_Company_Hierarchies`
  - `Exclude_Matrix_Organizations`
  - `Exclude_Supervisory_Organizations`
  - `Include_Roles`
- Response Filter Exclusion List: No default list.

b. Polling Job profile



- Poll Job Profile: Select enable for polling the Job profile information.

- Response Filter Inclusion List: The default option to pull the worker are as follows:
  Skip this option if you do not need any information.
  - `Include_Job_Profile_Compensation_Data`
  - `Include_Job_Profile_Basic_Data`

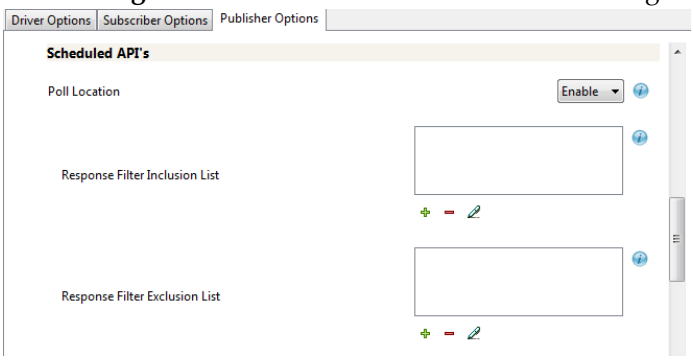
- Response Filter Exclusion List: No default list.

Poll Interval: Number of minutes between checks for available id's to process. This is applicable for worker and job profile both.

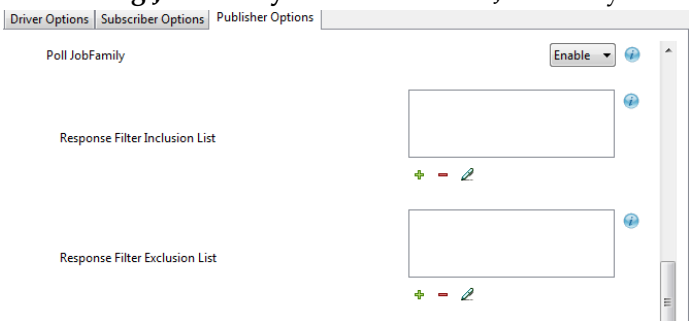
"No Request Criteria" for Initial Migration: To poll all records during initial migration, select the "Yes". Select "Poll Job profile" or "Poll Worker" as per business needs. It should be defined as false during normal operation.

- **Scheduled API:** API does not allow to poll data such as job family, location, organization, on basis of workday transition log. In this case polling the data changes in certain interval is not possible. Scheduling the night job is the best option to poll all the updated information.

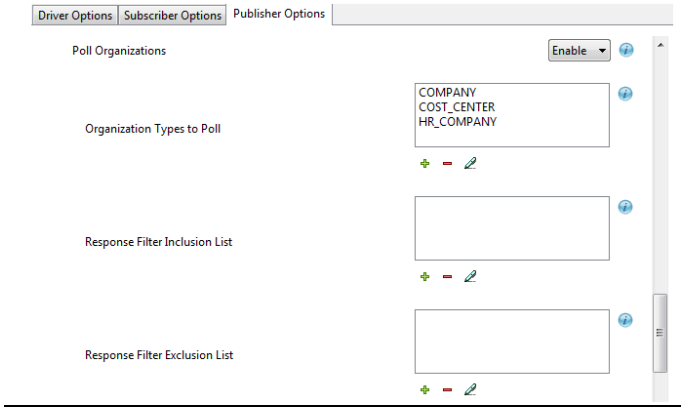
  a. **Polling Location:** Select to enable Location Polling.



  b. **Polling Job Family**: Select to enable Job Family Polling.

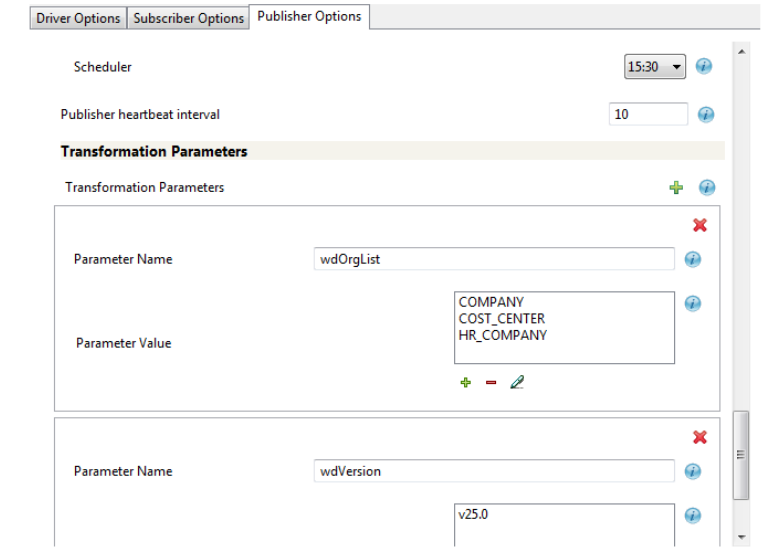


  c. **Polling Organization**: Select to enable Organization Polling.



d. **Polling Photo**: Select to enable Worker Photo.

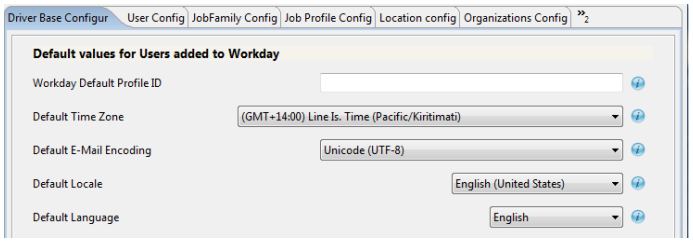
e. **Scheduling Job**: Select time to run the scheduled jobs (30 minutes interval)



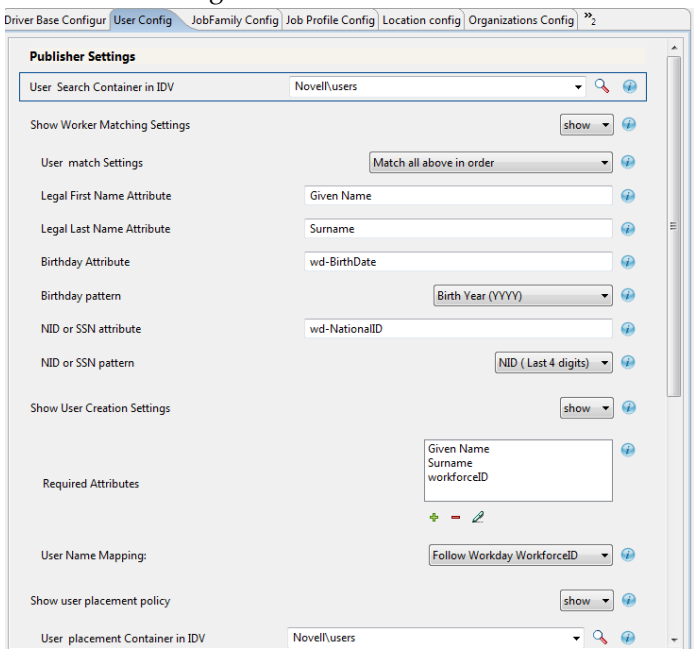
- Parameter Name: wdVersion (Do not change it)
  Value: Workday version: for Example v25.0
- Parameter Name: wdOrgList (Do not change it)
  Value: Organization Type (Configurable item in workday- Need to configure as per workday installation)
  a. COMPANY
  b. COST_CENTER
  c. HR_COMPANY

3.1.3.2Driver Configuration- Global Configuration Values (GCVs).

- **GCV** - Driver Base Configuration: Regional effect is planned but not yet configured on this version.



- **GCV**: User Configuration:



User match setting: Select a method for matching the user in IDV. Select Custom if you want your own policy. The system provides the following options to match the user under publisher matching policy.

- `Match Workforce ID`
- `Match user ID ( CN)`
- `Match Given Name, Surname , NID, Birthdate`
- `Match on Given Name ,Surname and NID`
- `Match Given Name, Surname and Birthdate`
- `Match all above in order`
- `Match Custom- Define yourself`

`Birthday Pattern:` The birthday pattern options are as follows:

- Birth year (YYYY)
- Birth Month and day (MMDD)
- Birthday Full (YYYYMMDD)

`NID or SSN Pattern:` The NID pattern options are as follows:

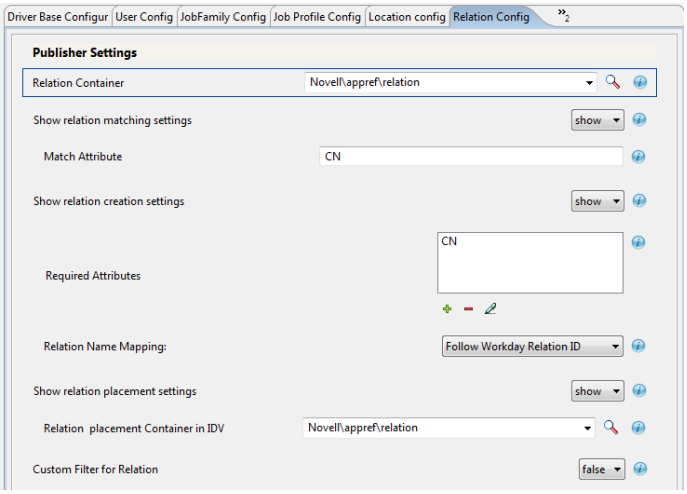
- Last 4 digits of NID
- NID Full

`Required attribute:` List of the required attributes for creating a new User object. Each of the attributes specified must be included in the Publisher filter.

`User Name Mapping:` Select a method for creating CN for `user.` The following options are available:

- Follow Workday Workforce ID
- Follow Workday User ID
- Follow Custom- define yourself

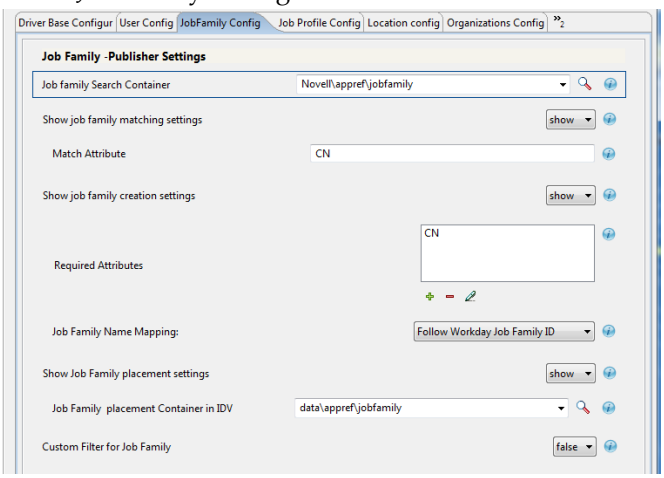
- **GCV**: Relation (Position) Configuration



`Relation Name Mapping:` Select a method for creating CN for Relation. The following options are available:

- Follow Workday Relation ID (Workforce ID-First Char of wd-WorkerIDType (E or C):PositionID).
  For example the CN for relation object for employee is “cn=12345-E:P012345” where,
  12345 is the workforceID
  -E is for employee and
  P012345 is the position ID
  The separator “-“ and “:” are not configurable.
- Follow Custom- this can be defined

- **GCV**: Job Family Configuration

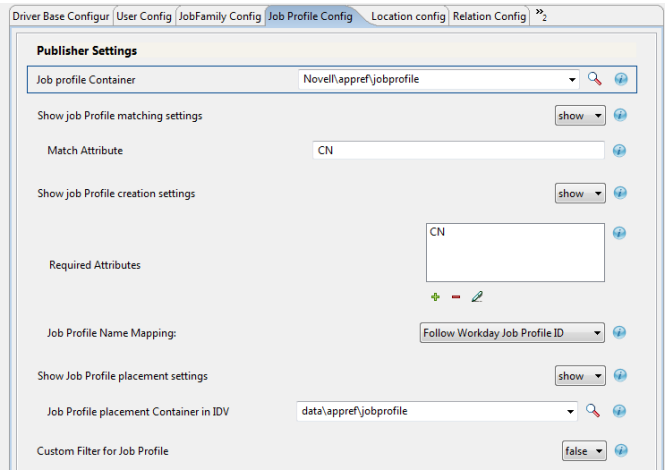


`Job Family Name Mapping:` Select a method for creating CN for Job family. The following options are available:

- Follow Workday Job Family ID

- Follow Custom- define yourself

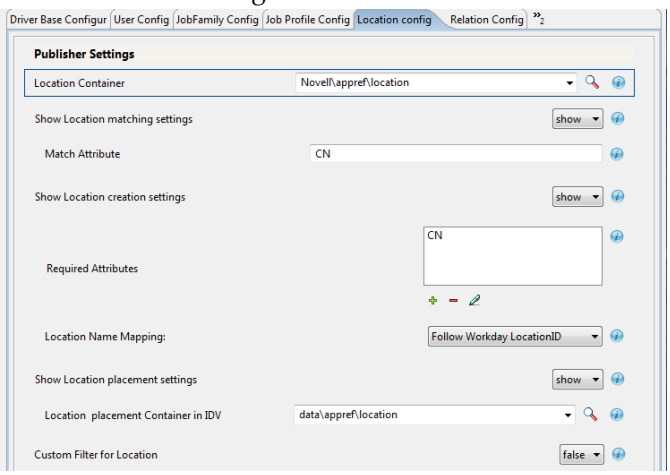
- **GCV**: Job Profile Configuration



`Job Profile Name Mapping:` Select a method for creating CN for Job profile. The following options are available:

- Follow Workday Job profile ID
- Follow Custom- define yourself

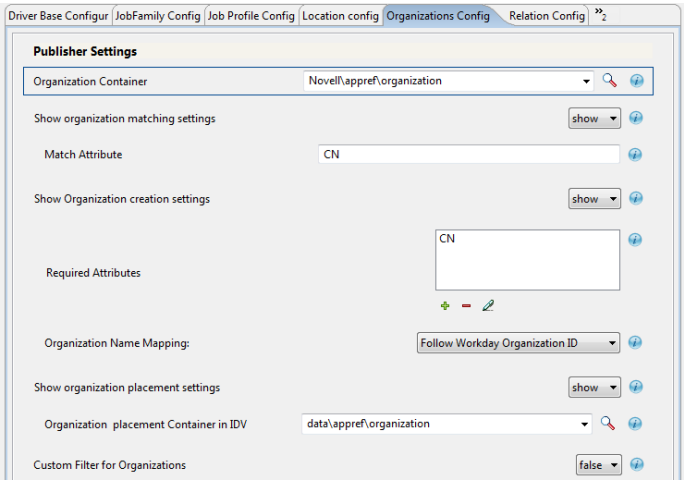
- **GCV**: Location Configuration



`Location Name Mapping:` Select a method for creating CN for Location. The following options are available:

- Follow Workday Location ID
- Follow Custom- define yourself

- **GCV**: Organization Configuration



`Organization Name Mapping:` Select a method for creating CN for Organization. The following options are available:

- Follow Workday Organization ID
- Follow Workday Organization Name
- Follow Custom- define yourself

- **GCV: Photo Configuration**

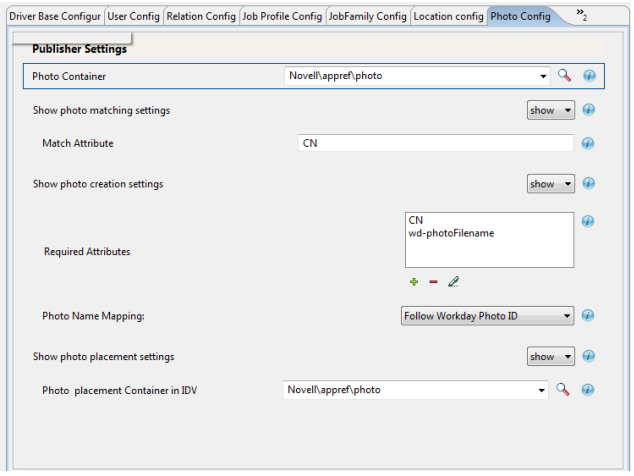
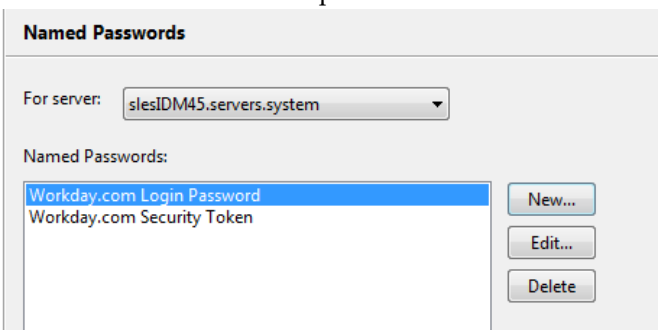


Photo Matching Configuration: The photo of the user is matched based on the CN of the user.

3.1.3.3 Driver Configuration- Named Password.

The driver has two named password defined for the workday.



Ensure that the correct password are applied under both the named passwords.

3.1.3.4 Customize the driver policies and filter:

The driver policies and filter control data flow between the Identity Vault and the application. Ensure that the policies and filters reflect your business needs. For instructions, see Chapter 4, "Schema Mapping," on page 23.

Perform the following actions if the Driver Properties page is not displayed in Designer:

1. Open your project.
2. In the Modeler, right-click the driver icon or the driver line, then select *Properties*.
3. Make any desired changes, then click *OK* to save the changes.
4. After the driver is create in Designer, it must be deployed to the Identity Vault. Proceed to Section 3.1.4, "Deploying the Driver Object," on page 19 to deploy the driver.

3.1.4 Deploying the Driver Object

After the driver object is created in Designer, it must be deployed to the Identity Vault.

1. In Designer, open your project.
2. In the Modeler, right-click the driver icon or the driver line, then click *Live* > *Deploy*.
3. If you are authenticated to the Identity Vault, skip to Step 5; otherwise, specify the following information:
   - **Host:** Specify the IP address or DNS name of the server hosting the Identity Vault.
   - **Username:** Specify the DN of the user object used to authenticate to the Identity Vault.
   - **Password:** Specify the user's password.
4. Click *OK*.
5. Click *Deploy*.
6. Click *OK*.
7. Click *Define Security Equivalence* to assign rights to the driver.

   The driver requires rights to objects within the Identity Vault. The Admin user object is most often used to supply these rights. However, you might want to create a DriversUser (for example) and assign security equivalence to that user.

   7a Click *Add*. Browse and select the object with the correct rights.

   7b Click *OK* twice.

   For more information about defining a Security Equivalent User in objects for drivers in the Identity Vault, see *Establishing a Security Equivalent User* in the *NetIQ Identity Manager Security Guide*.
8. Click *Exclude Administrative Roles* to exclude users that should not be synchronized.

   You should exclude any administrative User objects (for example, Admin and DriversUser) from synchronizing.

   8a Click *Add* and browse to select the user object you want to exclude.

   8b Click *OK*.

   8c Repeat Step 8a and Step 8b for each object you want to exclude.

   8d Click *OK*.

9 Click *OK*.

3.1.5 Starting the Driver

When a driver is created, it is stopped by default. To make the driver work, you must start the driver and cause events to occur. Identity Manager is an event-driven system, so after the driver is started, it won't do anything until an event occurs.

To start the driver:

1 In Designer, open your project.

2 In the Modeler, right-click the driver icon or the driver line, then select *Live* > *Start Driver*.

The driver cannot initialize completely unless it successfully connects to the .NET Remote Loader and loads the Workday driver shim.

For information about management tasks for the driver, see Chapter 7, "Managing the Driver," on page 29.

3.2 Activating the Driver

In order to activate the Workday driver, first activate the Metadirectory engine, and then activate the driver by using the separate Workday activation key. If you create the driver in a driver set that has not been activated, then you must activate the Metadirectory engine and the driver within 90 days. Else, the driver stops working.

If driver activation has expired, the following error message is displayed in the ndstrace window:

```
DirXML Log Event -------------------
Driver: \META-RHEL6\system\DriverSet\eDirDriver-BulkOperations
Channel: Subscriber
Status: Error
Message: Code(-9075) Shutting down because DirXML engine evaluation period
has expired. Activation is required for further use.
```

In order to use the driver, you must reactivate it.

For more information on activation, refer to "Activating Identity Manager" in the *NetIQ Identity Manager Setup Guide*.

3.3 Adding Packages to an Existing Driver

You can add new functionalities to an existing driver by adding new packages to an existing driver. Perform the following actions to add packages:

1 Right-click the driver, then click *Properties*.

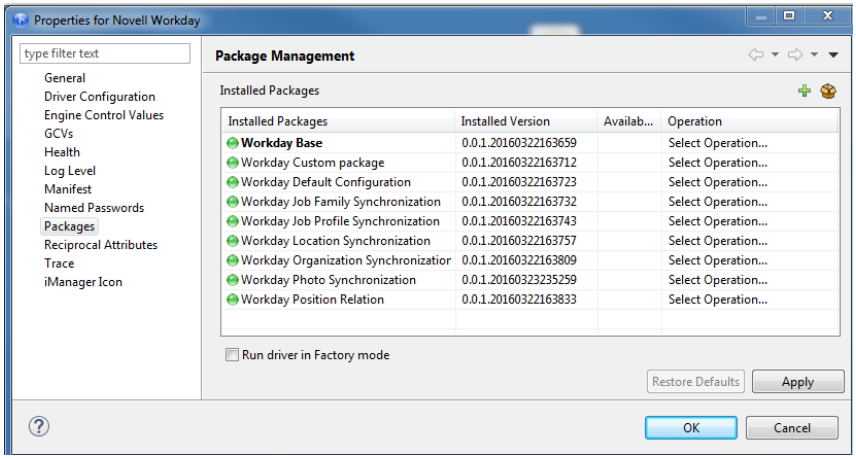
2 Click *Packages*, then click the *Add Packages* icon .

3 Select the packages to install. If the list is empty, it indicates that there are no available packages to install.

4 (Optional) Deselect the *Show only applicable package versions* option, if you want to see all available packages for the driver, and then click *OK*.

This option is only displayed on drivers. By default, only the packages that can be installed on the selected driver are displayed.

5 Click *Apply* to install all the listed packages with the Install operation.



6 (Conditional) Enter the fields with appropriate information to install the package you selected for the driver and click *Next*.

7 Click *Finish*.

8 Click *OK*.

9 Repeat Step 1 through Step 8 for each driver where you want to add the new packages.

4 Schema Mapping & filter settings

4.1 Schema Mapping

Table 4-1 lists Identity Vault user attributes that are mapped to the Workday user attributes. The default mappings are listed in the following table:

Table 4-1 *Mapped User Attributes when configured in the Workday*

class-name	nds-name	app-name
	User	**User**
User	C	wd-Country
User	CN	CN
User	Company	COMPANY_Name
User	Facsimile Telephone Number	wd-WorkFax
User	Generational Qualifier	wd-LegalGenerationQualifier
User	Given Name	wd-LegalFirstName
User	homeZipCode	wd-HomePostalCode
User	Initials	wd-LegalMiddleName
User	Internet EMail Address	wd-InternetEMailAddress
User	isManager	wd-isManager
User	JobCode	wd-JobProfileID
User	L	wd-LocationName
User	managerWorkforceID	wd-ManagerWorkforceID
User	mobile	wd-WorkMobile
User	nspmDistributionPassword	password
User	OU	COST_CENTER_Name
User	personalTitle	wd-LegalPersonalTitle
User	Physical Delivery Office Name	wd-City
User	Postal Code	wd-PostalCode
User	S	wd-State
User	SA	wd-StreetAddress
User	Surname	wd-LegalLastName
User	Telephone Number	wd-WorkTelephoneNumber
User	Title	wd-BusinessTitle
User	wd-BirthDate	wd-BirthDate
User	wd-BusinessAddressLine1	wd-BusinessAddressLine1
User	wd-BusinessCity	wd-BusinessCity
User	wd-BusinessCountry	wd-BusinessCountry

User	wd-BusinessPostalcode	wd-BusinessPostalcode
User	wd-BusinessState	wd-BusinessState
User	wd-C-Active	wd-C-Active
User	wd-C-ActivePositionIDs	wd-C-ActivePositionIDs
User	wd-C-Hiredate	wd-C-Hiredate
User	wd-C-Home_Countries	wd-C-Home_Countries
User	wd-C-Host_Countries	wd-C-Host_Countries
User	wd-C-International_Assignment	wd-C-International_Assignment
User	wd-COMPANY_Code	COMPANY_Code
User	wd-COMPANY_RefID	COMPANY_RefID
User	wd-C-OriginalHiredate	wd-C-OriginalHiredate
User	wd-COST_CENTER_Code	COST_CENTER_Code
User	wd-COST_CENTER_RefID	COST_CENTER_RefID
User	wd-C-Rehire	wd-C-Rehire
User	wd-C-Retired	wd-C-Retired
User	wd-C-Terminated	wd-C-Terminated
User	wd-C-TerminationDate	wd-C-TerminationDate
User	wd-E-Active	wd-E-Active
User	wd-E-ActivePositionIDs	wd-E-ActivePositionIDs
User	wd-E-Hiredate	wd-E-Hiredate
User	wd-E-Home_Countries	wd-E-Home_Countries
User	wd-E-Host_Countries	wd-E-Host_Countries
User	wd-E-International_Assignment	wd-E-International_Assignment
User	wd-E-OriginalHiredate	wd-E-OriginalHiredate
User	wd-E-Rehire	wd-E-Rehire
User	wd-E-Retired	wd-E-Retired
User	wd-E-Terminated	wd-E-Terminated
User	wd-E-TerminationDate	wd-E-TerminationDate
User	wd-HomeCity	wd-HomeCity
User	wd-HomeCountry	wd-HomeCountry
User	wd-HomeFax	wd-HomeFax
User	wd-HomeInternetEMailAddress	wd-HomeInternetEMailAddress
User	wd-HomeMobile	wd-HomeMobile
User	wd-HomeState	wd-HomeState
User	wd-HomeStreetAddress	wd-HomeStreetAddress
User	wd-HomeTelephoneNumber	wd-HomeTelephoneNumber
User	wd-HR_COMPANY_Code	HR_COMPANY_Code
User	wd-HR_COMPANY_Name	HR_COMPANY_Name
User	wd-HR_COMPANY_RefID	HR_COMPANY_RefID
User	wd-JobGroupReference	wd-JobGroupReference
User	wd-JobProfileName	wd-JobProfileName
User	wd-LocationID	wd-LocationID
User	wd-NationalID	wd-NationalID
User	wd-PayRateType	wd-PayRateType

User	wd-positioneffectiveDate	wd-positioneffectiveDate
User	wd-PositionEndDate	wd-PositionEndDate
User	wd-PositionID	wd-PositionID
User	wd-PositionstartDate	wd-PositionstartDate
User	wd-PositionTimeType	wd-PositionTimeType
User	wd-PositionTitle	wd-PositionTitle
User	wd-PreferredFirstName	wd-PreferredFirstName
User	wd-PreferredGenerationQualifier	wd-PreferredGenerationQualifier
User	wd-PreferredLastName	wd-PreferredLastName
User	wd-PreferredMiddleName	wd-PreferredMiddleName
User	wd-PreferredPersonalTitle	wd-PreferredPersonalTitle
User	wd-WorkerIDType	wd-WorkerIDType
User	wd-WorkerType	wd-WorkerType
User	workforceID	workforceID

Table 4-2 lists Identity Vault Relation attributes that are mapped to the Workday position attributes. The default mappings are listed in the following table:

NOTE: You can remap the same-type attributes.

Table 4-2 *Mapped Relation Attributes when configured in the Workday*

class-name	nds-name	app-name
	wd-Relation	**wd-Relation**
wd-Relation	COMPANY_Code	COMPANY_Code
wd-Relation	COMPANY_Name	COMPANY_Name
wd-Relation	COMPANY_RefID	COMPANY_RefID
wd-Relation	COST_CENTER_Code	COST_CENTER_Code
wd-Relation	COST_CENTER_Name	COST_CENTER_Name
wd-Relation	COST_CENTER_RefID	COST_CENTER_RefID
wd-Relation	HR_COMPANY_Code	HR_COMPANY_Code
wd-Relation	HR_COMPANY_Name	HR_COMPANY_Name
wd-Relation	HR_COMPANY_RefID	HR_COMPANY_RefID
wd-Relation	L	wd-LocationName
wd-Relation	managerWorkforceID	wd-ManagerWorkforceID
wd-Relation	Title	wd-BusinessTitle
wd-Relation	wd-BusinessAddressLine1	wd-BusinessAddressLine1
wd-Relation	wd-BusinessCity	wd-BusinessCity
wd-Relation	wd-BusinessCountry	wd-BusinessCountry
wd-Relation	wd-BusinessPostalcode	wd-BusinessPostalcode
wd-Relation	wd-BusinessState	wd-BusinessState
wd-Relation	wd-JobClassificationType	wd-JobClassificationType
wd-Relation	wd-JobGroupReference	wd-JobGroupReference
wd-Relation	wd-JobProfileName	wd-JobProfileName

wd-Relation	wd-LocationID	wd-LocationID
wd-Relation	wd-PayRateType	wd-PayRateType
wd-Relation	wd-PositionEffectiveDate	wd-PositionEffectiveDate
wd-Relation	wd-PositionEndDate	wd-PositionEndDate
wd-Relation	wd-PositionID	wd-PositionID
wd-Relation	wd-PositionstartDate	wd-PositionstartDate
wd-Relation	wd-PositionTimeType	wd-PositionTimeType
wd-Relation	wd-PositionTitle	wd-PositionTitle
wd-Relation	wd-Primary	wd-Primary
wd-Relation	wd-relationID	wd-relationID
wd-Relation	wd-WorkerIDType	wd-WorkerIDType
wd-Relation	wd-WorkerType	wd-WorkerType
wd-Relation	workforceID	workforceID
wd-Relation	wd-JobProfileID	wd-JobProfileID

Table 4-3 lists Identity Vault Job profile attributes that are mapped to the Workday job profile attributes. The default mappings are listed in the following table:

NOTE: You can remap the same-type attributes.

Table 4-3 *Mapped job profile Attributes when configured in the Workday*

Class Name	NDS-name	APP-name
	wd-Job	**wd-Job**
wd-Job	wd-CompensationGradeID	wd-CompensationGradeID
wd-Job	wd-CompensationGradeProfileID	wd-CompensationGradeProfileID
wd-Job	wd-Inactive	wd-Inactive
wd-Job	wd-JobCode	wd-JobCode
wd-Job	wd-JobFamilyID	wd-JobFamilyID
wd-Job	wd-JobProfileID	wd-JobProfileID
wd-Job	wd-JobTitle	Job_Title

Table 4-4 lists Identity Vault Job family attributes that are mapped to the Workday job family attributes. The default mappings are listed in the following table:

NOTE: You can remap the same-type attributes.

Table 4-4 *Mapped job family Attributes when configured in the Workday*

Class Name	NDS-name	APP-name
	wd-Jobfamily	**wd-Jobfamily**
wd-Jobfamily	wd-Inactive	wd-Inactive
wd-Jobfamily	wd-JobFamilyID	wd-JobFamilyID
wd-Jobfamily	wd-JobFamilyName	wd-JobFamilyName

Table 4-5 lists Identity Vault Location attributes that are mapped to the Workday location attributes. The default mappings are listed in the following table:

NOTE: You can remap the same-type attributes.

Table 4-5 *Mapped location Attributes when configured in the Workday*

Class Name	NDS-name	APP-name
	wd-Location	**wd-Location**
wd-Location	wd-AddressType	Address_type
wd-Location	wd-BusinessAddressLine1	wd-BusinessAddressLine1
wd-Location	wd-BusinessCity	wd-BusinessCity
wd-Location	wd-BusinessCountry	wd-BusinessCountry
wd-Location	wd-BusinessPostalcode	wd-BusinessPostalcode
wd-Location	wd-BusinessState	wd-BusinessState
wd-Location	wd-Inactive	wd-Inactive
wd-Location	wd-LocationID	wd-LocationID
wd-Location	wd-LocationName	wd-LocationName
wd-Location	wd-LocationUsageID	wd-LocationUsageID

Table 4-6 lists Identity Vault organization attributes that are mapped to the Workday organization attributes. The default mappings are listed in the following table:

NOTE: You can remap the same-type attributes.

Table 4-5 *Mapped organization Attributes when configured in the Workday*

Class Name	NDS-name	APP-name
	wd-organization	**wd-organization**
wd-organization	wd-Inactive	wd-Inactive
wd-organization	wd-OrganizationCode	wd-OrganizationCode
wd-organization	wd-OrganizationID	wd-OrganizationID
wd-organization	wd-OrganizationName	wd-OrganizationName
wd-organization	wd-OrganizationSubType	wd-OrganizationSubType
wd-organization	wd-OrganizationType	wd-OrganizationType

Table 4-7 lists Identity Vault user attributes for photo that are mapped to the Workday user's photo attributes.

Table 4-5 *Mapped user's photo Attributes when configured in the Workday*

Class Name	NDS-name	APP-name
	wd-Photo	**wd-Photo**
wd-Photo	photo	photo
wd-Photo	wd-photoFilename	wd-photoFilename
wd-Photo	wd-photoID	wd-photoID

4.1 Filter Settings

Table 4-8 lists Identity Vault Filter settings in the driver. The Workday is the authoritative source for almost all attributes except user ID and Email address which are generated in the IDV.

Table 4-8 *Driver filter settings for default configuration*

Filter-attr attr-name	Merge-authority	Publisher	Publisher-optimize-modify	Subscriber
User				
C	app	sync	true	ignore
CN	edir	notify	true	notify
co	app	sync	true	reset
company	app	sync	true	reset
costCenter	app	sync	true	notify
costCenterDescription	app	sync	true	reset
employeeStatus	app	sync	true	notify
employeeType	app	sync	true	notify
Generational Qualifier	app	sync	true	reset
Given Name	app	sync	true	reset
Initials	app	sync	true	reset
Internet EMail Address	edir	sync	true	sync
L	app	sync	true	reset
managerWorkforceID	app	sync	true	reset
OU	app	sync	true	reset
personalTitle	app	sync	true	reset
photo	app	sync	true	reset
Physical Delivery Office Name	app	sync	true	reset
Postal Code	app	sync	true	reset
S	app	sync	true	reset
SA	app	sync	true	reset
Surname	app	sync	true	reset
Telephone Number	app	sync	true	reset
Title	app	sync	true	reset
uniqueID	app	notify	true	ignore
wd-Active	app	sync	true	reset
wd-AddressType	app	sync	true	reset
wd-BirthDate	app	sync	true	reset
wd-BusinessAddressLine1	app	sync	true	reset
wd-BusinessCity	app	sync	true	reset
wd-BusinessCountry	app	sync	true	reset
wd-BusinessPostalcode	app	sync	true	reset

wd-BusinessState	app	sync	true	reset
wd-CompanyName	app	sync	true	reset
wd-Hiredate	app	sync	true	reset
wd-JobClassificationType	app	sync	true	reset
wd-JobGroupReference	app	sync	true	reset
wd-JobProfileID	app	sync	true	reset
wd-JobProfileName	app	sync	true	reset
wd-LocationID	app	sync	true	reset
wd-NationalID	app	sync	true	reset
wd-OriginalHiredate	app	sync	true	reset
wd-PayRateType	app	sync	true	reset
wd-photoFilename	app	sync	true	reset
wd-PositionID	app	sync	true	reset
wd-PositionstartDate	app	sync	true	reset
wd-PositionTimeType	app	sync	true	reset
wd-PreferredFirstName	app	sync	true	reset
wd-PreferredLastName	app	sync	true	reset
wd-PreferredMiddleName	app	sync	true	reset
wd-Rehire	app	sync	true	reset
wd-Retired	app	sync	true	reset
wd-Terminated	app	sync	true	reset
wd-TerminationDate	app	sync	true	reset
wd-WorkerIDType	app	sync	true	reset
workforceID	app	sync	true	reset
departmentNumber	app	sync	true	reset
wd-HomeCity	app	sync	true	reset
wd-HomeCountry	app	sync	true	reset
wd-HomeFax	app	sync	true	reset
wd-HomeInternetEMailAddress	app	sync	true	reset
wd-HomeMobile	app	sync	true	reset
wd-HomeState	app	sync	true	reset
wd-HomeStreetAddress	app	sync	true	reset
wd-HomeTelephoneNumber	app	sync	true	reset
wd-PositionTitle	app	sync	true	reset
homeZipCode	app	sync	true	reset
jobCode	app	sync	true	reset
mobile	app	sync	true	reset
Facsimile Telephone Number	app	sync	true	reset
O	app	sync	true	notify
wd-HR_COMPANY_Name	app	sync	true	reset
wd-HR_COMPANY_Code	app	sync	true	reset
wd-PositionEffectiveDate	app	sync	true	reset
DirXML-HireDateStr	app	sync	true	reset
THLastHireDateStr	app	sync	true	reset

DirXML-TerminationDateStr	app	sync	true	reset
wd-ActivePositionIDs	app	sync	true	reset
wd-C-Active	app	sync	true	reset
wd-C-Hiredate	app	sync	true	reset
wd-C-OriginalHiredate	app	sync	true	reset
wd-C-Rehire	app	sync	true	reset
wd-C-Retired	app	sync	true	reset
wd-C-Terminated	app	sync	true	reset
wd-C-TerminationDate	app	sync	true	reset
wd-E-Active	app	sync	true	reset
wd-E-Hiredate	app	sync	true	reset
wd-E-OriginalHiredate	app	sync	true	reset
wd-E-Rehire	app	sync	true	reset
wd-E-Retired	app	sync	true	reset
wd-E-Terminated	app	sync	true	reset
wd-E-TerminationDate	app	sync	true	reset
wd-C-ActivePositionIDs	app	sync	true	reset
wd-E-ActivePositionIDs	app	sync	true	reset
wd-PositionEndDate	app	sync	true	reset
wd-C-Home_Countries	app	sync	true	reset
wd-C-Host_Countries	app	sync	true	reset
wd-C-International_Assignment	app	sync	true	reset
wd-COMPANY_RefID	app	sync	true	reset
wd-COST_CENTER_RefID	app	sync	true	reset
wd-E-Home_Countries	app	sync	true	reset
wd-E-Host_Countries	app	sync	true	reset
wd-E-International_Assignment	app	sync	true	reset
wd-HR_COMPANY_RefID	app	sync	true	reset
wd-PreferredGenerationQualifier	app	sync	true	reset
wd-PreferredPersonalTitle	app	sync	true	reset
wd-WorkerType	app	sync	true	reset
isManager	app	sync	true	reset
wd-Jobprofile				
CN	default	sync	true	notify
wd-CompensationGradeID	app	sync	true	reset
wd-CompensationGradeProfileID	app	sync	true	reset
wd-Inactive	app	sync	true	reset
wd-JobCode	app	sync	true	reset
wd-JobFamilyID	app	sync	true	reset
wd-JobTitle	app	sync	true	reset
wd-JobProfileID	app	sync	true	reset
wd-Location				

CN	default	sync	true	notify
wd-AddressType	app	sync	true	reset
wd-BusinessAddressLine1	app	sync	true	reset
wd-BusinessCity	app	sync	true	reset
wd-BusinessCountry	app	sync	true	reset
wd-BusinessPostalcode	app	sync	true	reset
wd-BusinessState	app	sync	true	reset
wd-Inactive	app	sync	true	reset
wd-LocationID	app	sync	true	reset
wd-LocationName	app	sync	true	reset
wd-LocationUsageID	app	sync	true	reset
wd-Jobfamily				
CN	default	sync	true	notify
wd-Inactive	app	sync	true	reset
wd-JobFamilyID	app	sync	true	reset
wd-JobFamilyName	app	sync	true	reset
wd-organization				
CN	default	sync	true	notify
wd-Inactive	app	sync	true	reset
wd-OrganizationCode	app	sync	true	reset
wd-OrganizationID	app	sync	true	reset
wd-OrganizationName	app	sync	true	reset
wd-OrganizationSubType	app	sync	true	reset
wd-OrganizationType	app	sync	true	reset
wd-Relation				
CN	default	sync	true	notify
L	app	sync	true	reset
managerWorkforceID	app	sync	true	reset
Title	app	sync	true	reset
wd-BusinessAddressLine1	app	sync	true	reset
wd-BusinessCity	app	sync	true	reset
wd-BusinessCountry	app	sync	true	reset
wd-BusinessPostalcode	app	sync	true	reset
wd-BusinessState	app	sync	true	reset
wd-JobClassificationType	app	sync	true	reset
wd-JobFamilyID	app	sync	true	reset
wd-JobGroupReference	app	sync	true	reset
wd-JobProfileName	app	sync	true	reset
wd-LocationID	app	sync	true	reset
wd-PayRateType	app	sync	true	reset
wd-PositionID	app	sync	true	reset

wd-PositionstartDate	app	sync	true	reset
wd-PositionTimeType	app	sync	true	reset
wd-Primary	app	sync	true	reset
wd-RelationID	app	sync	true	reset
wd-WorkerType	app	sync	true	reset
workforceID	app	sync	true	reset
wd-PositionTitle	app	sync	true	reset
wd-PositionEffectiveDate	app	sync	true	reset
wd-WorkerIDType	app	sync	true	reset
wd-PositionEndDate	app	sync	true	reset
wd-COMPANY_ Code	app	sync	true	reset
wd-COMPANY_Name	app	sync	true	reset
wd-COMPANY_RefID	app	sync	true	reset
wd-COST_CENTER_Code	app	sync	true	reset
wd-COST_CENTER_Name	app	sync	true	reset
wd-COST_CENTER_RefID	app	sync	true	reset
wd-HR_COMPANY_Code	app	sync	true	reset
wd-HR_COMPANY_Name	app	sync	true	reset
wd-HR_COMPANY_RefID	app	sync	true	reset
jobCode	app	sync	true	reset
wd-Photo				
CN	default	sync	true	notify
photo	app	sync	true	reset
wd-photoFilename	app	sync	true	reset
wd-photoID	app	sync	true	reset

5 Securing Communication

If the remote Web service you access allows HTTPS connections, you can configure the driver to take advantage of this increased security.

IMPORTANT: Ensure that the keystore of the certificates is a Java keystore as only certificates from Java keystore are accepted.

The Subscriber channel sends information from the Identity vault to Workday. To establish a secure connection for the Subscriber channel, you require a trust store containing a certificate issued by the certificate authority that signed the server's certificate.

Import this certificate into a trust store using Java's keytool. For more information on keytool, see Keytool - Key and Certificate Management Tool.

1. Import the certificate into the trust store or create a new trust store by entering the following command using command prompt:

   `keytool -import -file` *`name_of_cert_file`* `-trustcacerts -noprompt -keystore` *`filename`* `-storepass` *`password`* For example:

   ```
   keytool -import -file tree_ca_root.b64 -trustcacerts -noprompt -keystore
   dirxml.keystore -storepass novell
   ```

2. Configure the Subscriber channel to use the trust store you created in Step 1:

   2a In iManager, in the *Roles and Tasks* view, click *Identity Manager* > *Identity Manager Overview*.

   2b Locate the driver set containing the Workday driver, after you click the driver's icon to display the Identity Manager Driver Overview page.

   2c On the Identity Manager Driver Overview page, click the driver's icon again, then scroll to the *Subscriber Settings*.

   2d In the *Keystore File* setting, specify the path to the trust store you created in Step 1.

   3 Click *Apply*, and then click *OK*.

6 Managing the Driver

As you work with the Workday driver, perform the following management tasks:

- Starting, stopping, and restarting the driver
- Viewing driver version information
- Using Named Passwords to securely store passwords associated with the driver
- Monitoring the driver's health status
- Backing up the driver
- Inspecting the driver's cache files
- Viewing the driver's statistics
- Using the DirXML Command Line utility to perform management tasks through scripts
- Securing the driver and its information

For more details about these tasks, see *NetIQ Identity Manager Common Driver Administration Guide*.

7 Troubleshooting the Driver

You can log Identity Manager Events by setting the log level 5 at the driver and also at remote loader. Using this log combination provides a tracking control at a very granular level.

This section contains the following information on error messages:

- Section 8.1, “Driver Shim Errors,” on page 31
- Section 8.2, “Driver Cache file and driver state settings
- Section 8.3, “Troubleshooting Driver Processes,”
- Section 8.4, “Migrating/Updating individual object from Workday,”

8.1 Driver Shim Errors

This identifies errors that might occur in the core driver shim. Error messages that contain a numerical code can have various messages, depending on the application or Web service.

8.2 Driver Cache file and Driver State settings:

As part of cache management, the shim develops sets of cache files. It compares the attribute value after conversion from SOAP response and passes only the changed value to the driver channel. The driver develops the cache file either on the server where IDM engine is running (in Native setup), or at the remote loader server where the driver shim is running on remote loader. You can delete these files in the case any of them are corrupted. After deletion, the driver redevelops these files. However, in this process, the driver loses all the caches and builds up cache again afresh. Following is an example of the remote loader setup cache files:

The Driver state setting includes information about the last poll timestamp and also pages fetches in the initial migration. Following is an example of the state files:

state__u5fTREEu5fSLES_system_driverset1_workdayu20v25.xml

The details of the file are as follows:

```
<init-params><publisher-state><mig-last-poll-timestamp-Worker-end>2015-12-01T21:05:51.869
</mig-last-poll-timestamp-Worker-end><last-poll-timestamp-JobProfile>2015-12-01T21:05:51.869
</last-poll-timestamp-JobProfile><mig-last-poll-timestamp-Worker-start>2015-12-01T21:04:41.372
</mig-last-poll-timestamp-Worker-start><migration_page_polled>0
</migration_page_polled><migration_total_page>0</migration_total_page><migration_entry_time>
2015-12-01T21:05:51.869</migration_entry_time><last-poll-timestamp-Worker>2015-12-01T21:05:51.321
</last-poll-timestamp-Worker></publisher-state></init-params>
```

You can reprocess all events by changing the date and time stamp in this file.

On the server, edit the DirXML-DriverStorage for changing the details of this file.

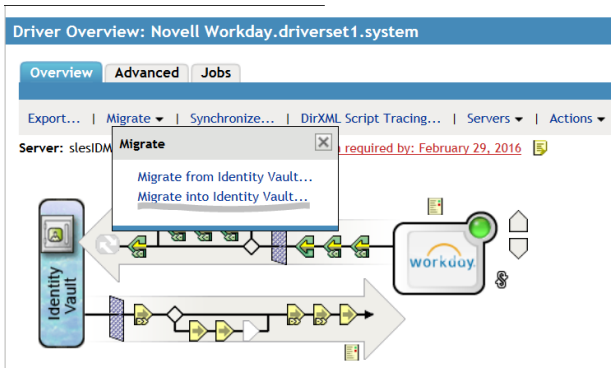
8.3 Troubleshooting Driver Processes

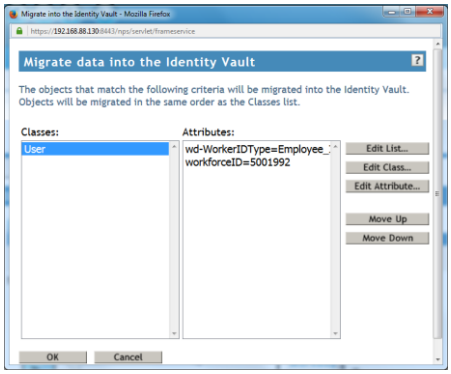
Viewing the driver processes are necessary to analyze unexpected behavior. To view the driver processing events, use DSTrace. This should be used only during testing and troubleshooting of the driver. Running DSTrace while the drivers are in production increases the utilization on the Identity Manager server. This causes slow event processing. For more information, see "Viewing Identity Manager Processes" in the *NetIQ Identity Manager Common Driver Administration Guide*.

8.4 Migrating Individual Object from Workday

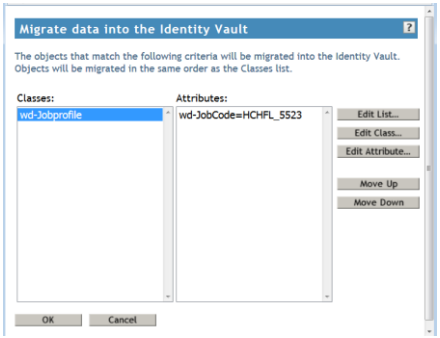
You can migrate individual user object such as employee or Contingent worker with relation (Position). You can also migrate other object such as job profile, job family, location, organization including cost center, company, HR Company etc. This process updates the IDV object with the latest information.

- To migrate the user with relation:
  - Use iManager "Migrate into Identity vault" option to migrate individual employee or contingent worker.
  - Select "edit List"
  - Select user as class and Select show all attributes
  - Select workforce ID and wd-workerIDType and provide the required data
  - Wd-workerIDType can be Employee_ID or Contingent_Worker_ID
  - Workforce ID is the unique ID in the workday.
  - Click ok to migrate the worker record



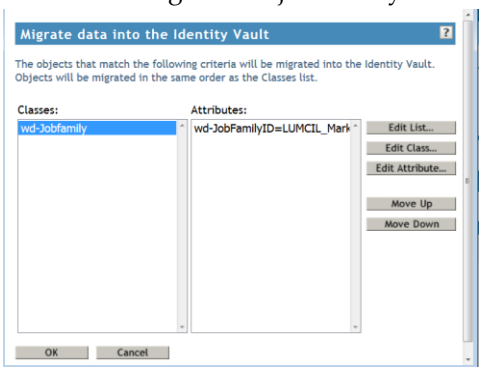


- To migrate job profile:
  - Use iManager "Migrate into Identity vault" option to migrate job profile
  - Select "edit List"
  - Select wd-Jobprofile as class and Select show all attributes
  - Select wd-JobCode and provide the wd-JobCode of the object to migrate
  - Click ok to migrate the job profile.

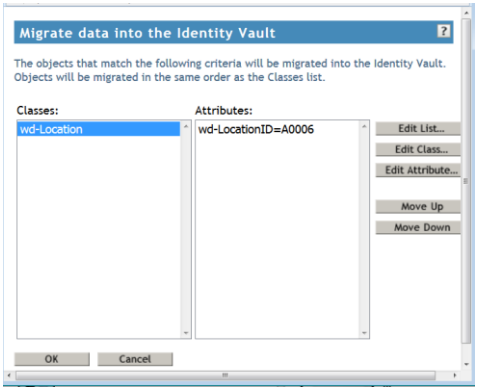


- To migrate job Family:
  - Use iManager "Migrate into Identity vault" option to migrate job family
  - Select "edit List"
  - Select wd-family as class and Select show all attributes
  - Select wd-JobFamilyID and provide the wd-JobFamilyID of the object to migrate

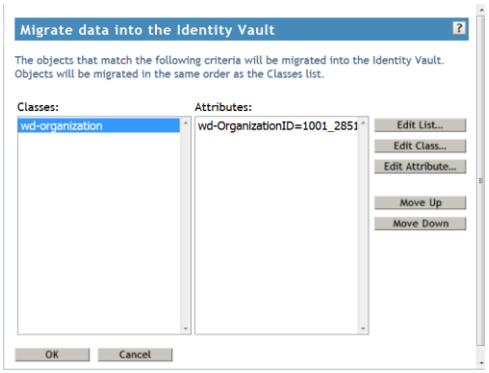
- Click ok to migrate the job Family.



- To migrate Location:
  - Use iManager "Migrate into Identity vault" option to migrate job family
  - Select "edit List"
  - Select wd-location as class and Select show all attributes
  - Select wd-LocationID and provide the wd-LocationID of the object to migrate
  - Click ok to migrate the Location

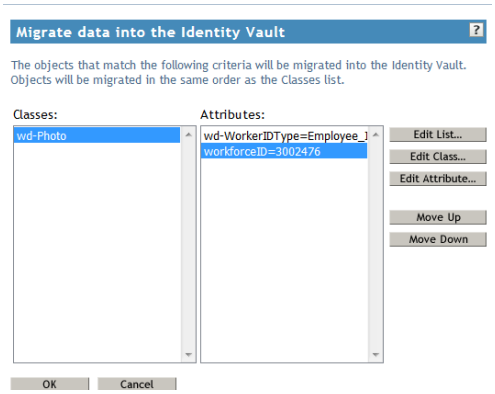


- Tp migrating Organization – Cost center, company, HR company:
  - Use iManager "Migrate into Identity vault" option to migrate job family
  - Select "edit List"
  - Select wd-organization as class and Select show all attributes
  - Select wd-OrganizationID and provide the wd-OrganizationID of the object to migrate
  - Click ok to migrate the organization



- To migrate user's photo:

- Use iManager "Migrate into Identity vault" option to migrate Photo
- Select "edit List"
- Select wd-photo as class and Select show all attributes
- Select wd-EmployeeID and provide the workforceID of the object to migrate
- Click ok to migrate the Photo



(A) Driver Properties

This section provides information about the Driver Configuration and Global Configuration Values properties for the Workday driver. These are the only unique properties for drivers. All other driver properties (Named Password, Engine Control Values, Log Level, and so forth) are common to all drivers. Refer to "Driver Properties" in the *NetIQ Identity Manager Common Driver Administration Guide* for information about the common properties.

The information is presented from the viewpoint of iManager. If a field is different in Designer, it is marked with a Designer icon.

- Section A.1, "Driver Configuration," on page 35
- Section A.2, "Global Configuration Values," on page 38

A.1 Driver Configuration

In iManager:

1. Click to display the Identity Manager Administration page.
2. Open the driver set that contains the driver whose properties you want to edit:
   - **2a** In the *Administration* list, click *Identity Manager Overview*.
   - **2b** If the driver set is not listed on the *Driver Sets* tab, use the *Search In* field to search for and display the driver set.
   - **2c** Click the driver set to open the Driver Set Overview page.
3. Locate the driver icon, then click the upper right corner of the driver icon to display the *Actions* menu.
4. Click *Edit Properties* to display the driver's properties page.

   By default, the Driver Configuration page is displayed.

In Designer:

1. Open a project in the Modeler.
2. Right-click the driver icon or line, then select click *Properties* > *Driver Configuration.*

The Driver Configuration options are divided into the following sections:

A.1.1 Driver Module

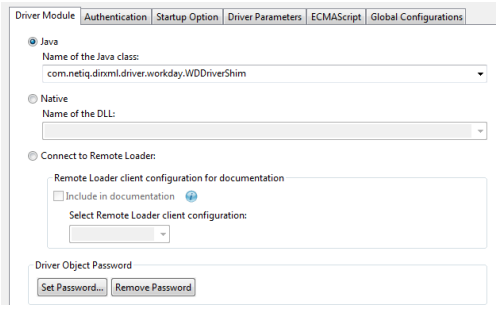
The driver module changes the driver from running locally to running remotely or the reverse.

Java: Used to specify the name of the Java class that is instantiated for the shim component of the driver. This class can be located in the `classes` directory as a class file, or in the `lib` directory as a `.jar` file. If this option is selected, the driver is running locally.

The Java class name is:

```
com.netiq.dirxml.driver.workday.WDDriverShim
```

Native: Used when driver is connecting directly from the server where IDM engine is installed.



Connect to Remote Loader: Used when the driver is connecting remotely to the connected system. Designer includes two suboptions:

- **Driver Object Password:** Specifies a password for the Driver object. If you are using the Remote Loader, you must enter a password on this page. Otherwise, the remote driver does not run. The Remote Loader uses this password to authenticate itself to the remote driver shim.
- **Remote Loader Client Configuration for Documentation:** Includes information on the Remote Loader client configuration when Designer generates documentation for the driver.

A.1.2Driver Object Password

Driver Object Password: Use this option to set a password for the driver object. If you are using the Remote Loader, you must enter a password on this page or the remote driver does not run. This password is used by the Remote Loader to authenticate itself to the remote driver shim.

A.1.3 Authentication

The authentication section stores the information required to authenticate to the connected system.

Authentication ID: This option is not used with the Workday driver.

Authentication Context: This option is not used with the Workday driver.

Remote Loader Connection Parameters: Used only if the driver is connecting to the application through the Remote Loader. The parameter to enter is `hostnamexxx.xxx.xxx.xxx portxxxx kmocertificatename`, when the host name is the IP address of the application server running the Remote Loader server and the port is the port the Remote Loader is listening on. The default port for the Remote Loader is 8090.

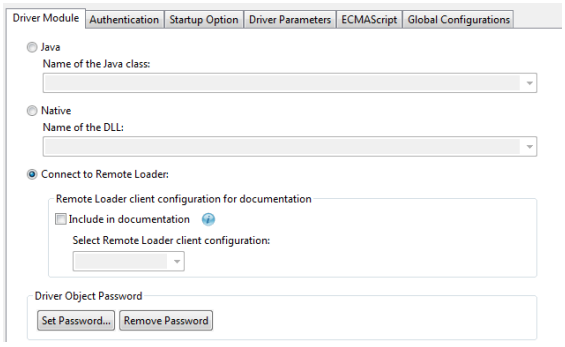
The `kmo` entry is optional. It is only used when there is an SSL connection between the Remote Loader and the Metadirectory engine.

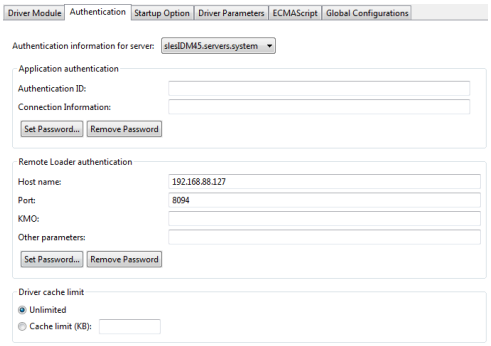
Example: `hostname10.0.0.1 port8090 kmoIDMCertificate`

Cache limit (KB): Specify the maximum event cache file size (in KB). If it is set to zero, the file size is unlimited. Click *Unlimited* to set the file size to unlimited in Designer.

Application Password: This option is not used with the Workday driver.

Remote Loader Password: Used only if the driver is connecting to the application through the Remote Loader. The password is used to control access to the Remote Loader instance. It must be the same password specified during the configuration of the Remote Loader on the connected system.





A.1.4 Startup Option

The Startup Option section allows you to set the driver state when the Identity Manager server is started.

Auto start: The driver starts every time the Identity Manager server is started.

Manual: The driver does not start when the Identity Manager server is started. The driver must be started through Designer or iManager.

Disabled: The driver has a cache file that stores all of the events. When the driver is set to Disabled, this file is deleted and no new events are stored in the file until the driver state is changed to Manual or Auto Start.

Do not automatically synchronize the driver: This option only applies if the driver is deployed and was previously disabled. If this is not selected, the driver re-synchronizes the next time it is started.

A.1.5 Driver Parameters

The Driver Parameters section lets you configure the driver-specific parameters. When you change driver parameters, you tune driver behavior to align with your network environment. The parameters are divided into the following categories:

Driver Settings

Workday Login URL: Specify the URL of the Workday Login Server based on your choice of Workday WSDL.

The default URL is https://www.Workday/services/Soap/u/18.0.

Workday Login ID: Specify the Login ID of the Workday administrator.

Ensure that you create a unique administrator user to be solely used by the Workday driver for authentication and specify that user in this parameter. If you specify the same user with which you

login and administer Workday, the driver ignores changes on the Publisher channel (loopback detection).

Workday Login Password: Specify the password for the Workday administrator.

If you need to clear the password, select *Remove existing password*, then click *Apply*.

Workday Security Token: Specify the security token for your login account at Workday.

Proxy host and port: When an HTTP proxy is used, specify the host address and the host port. For example: 192.10.1.3:18180.

Set Proxy Authentication parameters: Select *Show* to display the proxy authentication parameters.

- **Proxy User ID:** Specify the username of the proxy user for authentication. Leave the field blank for anonymous authentication.
- **Proxy User Password:** Specify the password of the proxy user, if proxy user authentication is used.

Truststore File: Specify the name and path of the keystore file containing the trusted certificates used when the remote server is configured to provide server authentication. For example: `c:\security\truststore`. Leave this field empty when server authentication is not used.

NOTE: A Workday client calling the Web service in the Publisher channel must specify a URL ending with a slash. For example, *http://1.1.1.1:9095/*. Without a context path (the slash), the driver does not process the request received.

(B) Trace Level

The driver supports the following trace levels:

Table B-1 *Supported Trace Levels*

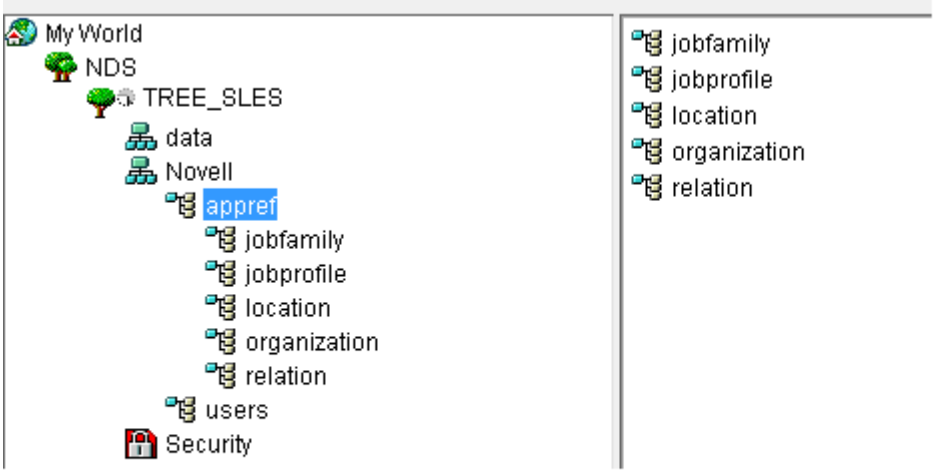
Level	Description
0	No debugging
1-2	Identity Manager messages. Higher trace levels provide more detail.
3	Previous level plus driver parameters, Remote Loader, driver shim, and driver connection messages
5	Previous level plus driver status log, driver security, driver schema, driver communication details, request and response XML, Workday API calls

For information about setting driver trace levels, see "Viewing Identity Manager Processes" in the *NetIQ Identity Manager Common Driver Administration Guide*.

(C) IDV Schema extension:

As part of solution, we need to extend the schema of eDirectory so that the Workday driver can create these additional objects in the IDV. The proposed schema extension in ldif and sch formats are available for download. The following classes are added in IDV.

- Auxiliary Class for User : wd-User
- Effective Class for Relation Objects: wd-Relation
- Effective Class for Relation Objects: wd-Jobfamily
- Effective Class for Relation Objects: wd-Jobprofile
- Effective Class for Relation Objects: wd-Location
- Effective Class for Relation Objects: wd-Organization
- Effective Class for Relation Objects: wd-Relation

(D) IDV proposed structure:

As part of solution, it is proposed to have a different container for different objects in IDV. The proposed structure is as follow: